Groupe d'études
Assurances

Rapport

La cyber-assurance

Par Valéria FAURE-MUNTIAN, Députée de la Loire et Présidente du Groupe d'études Assurances de l'Assemblée nationale

Avec l'assistance de
Romain DEWAELE
Collaborateur parlementaire

Assemblée Nationale

2021

Remerciements

Je tiens à remercier vivement Monsieur Jérôme Notin, Directeur général du Groupement d'intérêt public Action contre la cybermalveillance (GIP ACYMA), pour la préface de ce rapport et pour son décryptage de la cyber-menace.

Je remercie également Monsieur Guillaume Poupard, Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), pour la qualité de nos échanges et pour son mot éclairant.

De même, j'adresse mes remerciements à Monsieur Lionel Corre, Sous-directeur des assurances à la Direction générale du Trésor (DGT) et son équipe, pour leur analyse de l'état des lieux.

Je souhaite aussi remercier l'Autorité de contrôle prudentiel et de résolution (ACPR) pour le partage de leur vision sur la cyber-assurance.

Je souhaite remercier l'ensemble des personnalités auditionnées et les contributeurs, dont la disponibilité et l'expertise ont particulièrement alimenté ma réflexion.

Enfin, j'adresse mes plus sincères remerciements à toute mon équipe, qui m'a accompagnée, soutenue et aidée tout au long de la production de ce rapport.

Synthèse

Le présent rapport entend dresser le kaléidoscope de la situation de la cyber-assurance en France, et proposer des voies d'amélioration jugées nécessaires dans un contexte toujours plus risqué pour les entreprises, qui peinent à se couvrir.

Dans un premier temps, le rapport préconise de clarifier et de définir les termes propres au champ du risque cyber, avant de délimiter une législation efficace susceptible de le réguler. D'une part, les définitions juridiques du cyber-risque, de la cyber-attaque doivent ainsi être adoptées. D'autre part, les régimes applicables au paiement des rançons, au paiement des amendes administratives et à l'activation des garanties assurantielles doivent être consacrés.

Dans un deuxième temps, le rapport entend garantir la résilience et la défense des entreprises et des collectivités françaises face à cette nouvelle menace. D'une part, en renforçant l'écosystème français de la cybersécurité, aujourd'hui éclaté, en renforçant l'influence et la coopération des différents acteurs privés et institutionnels. D'autre part, en sensibilisant les entreprises et les collectivités au minimum des prérequis pour couvrir leur vulnérabilité, toujours croissante.

Enfin, dans le but de dynamiser le marché de la cyber-assurance, ce rapport contient des voies d'amélioration de l'offre pour une couverture suffisamment importante afin de sécuriser notre économie. Aujourd'hui, le marché de l'offre s'avère déséquilibré et concentré, avec une couverture inégale, alors même qu'il s'agirait d'un vecteur indispensable de prévention. Face à ce constat, il paraît nécessaire de mieux organiser le marché en renforçant l'offre auprès des entreprises, et en développant des solutions innovantes. Un équilibre doit être recherché en associant une demande sensibilisée, alerte et soucieuse de sa sécurité, avec une offre cohérente, adaptée et suffisamment compétitive pour convaincre les entreprises.

Sommaire

Remerciements 2

Synthèse 3

Préface par Monsieur Jérôme Notin, Directeur général du GIP ACYMA (Groupement d'intérêt public Action contre la cybermalveillance) 5

Introduction 6

Mot de Monsieur Guillaume Poupard, Directeur général de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) 8

Propositions 9

I) Une effectivité juridique à garantir 10

1) Des définitions à clarifier 10

2) Des régimes à optimiser 12

II) Une résilience à encourager 16

1) Un écosystème à renforcer 16

2) Des acteurs à sensibiliser 20

III) Une offre assurantielle à dynamiser 22

1) Un marché jugé insuffisant 22

2) Des pistes d'évolution 25

Conclusion 27

Annexes 28

Auditions 35

Préface par Monsieur Jérôme Notin, Directeur général du GIP ACYMA (Groupement d'intérêt public Action contre la cybermalveillance)

L'explosion des usages numériques ces dernières années, qui s'est encore accentuée avec la crise sanitaire par le télétravail massif, le téléenseignement, le commerce en ligne, a vu en corollaire une recrudescence sans précédent des faits de cybermalveillance. Contrairement à l'image souvent véhiculée, les cyber-criminels ne sont plus aujourd'hui les seuls adolescents immatures que l'on peut imaginer. Ils s'organisent sur le darknet en équipes très structurées et compétentes pour maximiser leurs profits. Leur seule idéologie est de chercher à gagner le plus d'argent possible, peu en importe les conséquences pour les victimes qui peuvent avoir leurs systèmes d'information chiffrés, pillés, sabotés etc. Particuliers, entreprises, collectivités, associations et mêmes hôpitaux et États, plus personne n'est aujourd'hui, et ne sera demain, épargné.

Se protéger pour soi, mais aussi pour les autres

Se protéger de la cybermalveillance c'est avant tout se protéger soi-même. Protéger son identité numérique, mais aussi ses moyens informatiques et de communication contre les différents types d'attaques qu'ils peuvent subir. Et avec l'interpénétration des usages numériques personnels et professionnels, se protéger soi-même c'est aussi protéger ses collègues, son entreprise, et ses administrés pour les collectivités. En effet, les conséquences d'un manque de respects des règles de bases de la cybersécurité à titre individuel ont des impacts sur le collectif. Cela met en danger son emploi et celui des autres salariés, voire notre résilience au niveau national si des attaques massives touchaient notre tissu économique : un blocage de 10 % des PME françaises deviendrait un problème de sécurité nationale.

Comment se protéger ?

Pour commencer à se protéger il faut déjà prendre conscience des risques pour en accepter les contraintes. Et ces risques sont réels : l'actualité le démontre quasi quotidiennement. Ce premier pas effectué, il faut comprendre qu'une très grande majorité des cyber-attaques pourrait être évitée si des mesures simples étaient respectées comme une bonne gestion des mots de passes, si les mises à jour de sécurité étaient régulièrement appliquées, si l'ensemble des données étaient régulièrement et convenablement sauvegardées.

La première action est donc de sensibiliser le plus massivement possible. La seconde est de régler la dette du niveau de cybersécurité qui peut parfois s'avérer lourde. Il faut donc prioriser ses actions techniques après avoir réalisé un état des lieux pour commencer par combler ses vulnérabilités les plus critiques. Pour cela, il faut savoir se faire accompagner par des spécialistes en cybersécurité comme les prestataires labellisés ExpertCyber que nous avons créé au sein de Cybermalveillance.gouv.fr.

Et ensuite ?

Une fois le cycle perpétuel et vertueux de la sensibilisation défini, une fois les mesures techniques et organisationnelles prises, reste à adresser le risque résiduel. Pour cela, nous avons besoin d'une offre assurantielle forte, qui soit adaptée aux contraintes et réalités du marché, et ceci quelle que soit la taille de la structure couverte, pouvant donc aller jusqu'aux particuliers. Cette offre doit être créée par le « marché », qui doit être lui-même être soutenu par une évolution de la législation dans le domaine de l'assurance.

Introduction

La peur, n'évite pas le danger. Cet adage populaire résume bien l'état du marché de l'assurance cyber en France. Démarrant sur les chapeaux de roues fin des années 2000, ce marché freine puis connait l'accident lors de la crise sanitaire. Le ratio sinistre à prime ayant été multiplié par deux entre 2019 et 2020.

En 2020 le risque cyber était la première menace pour l'économie française d'après le baromètre annuel des risques édité par Allianz[1].

Qualifié de risque systémique il est considéré même comme inassurable par certains acteurs du marché français.

Éducation, transports, énergie, communication, culture, urbanisme, industrie, santé, agriculture… Nos actes quotidiens, professionnels comme personnels, sont de plus en plus digitalisés, numérisés et dématérialisés. Si ce processus était déjà en cours depuis quelques années, la crise sanitaire due à la pandémie de Covid-19 a accéléré cette tendance.

Assurément, le maintien des interactions sociales et de l'activité économique fut, et demeurent pour partie, dépendants des outils numériques. Dès lors la surface ciblée par les cyber-attaquants fut décuplée. De même, de la relation aux clients à la chaine de production de valeurs, le numérique bouleverse le quotidien des entreprises et devient un moyen indispensable de compétitivité, de croissance et d'innovation.

Espionnage, fausses informations, sabotage, vols d'information, rançongiciels… L'échiquier des cyber-attaques est large, en constante évolution, et de plus en en plus intense.

Particuliers, petites entreprises, grands groupes, administrations, collectivités…Tout le monde peut être ciblé et personne n'est épargné par les cyber-attaques. États, mercenaires, criminels, cyber-attaquants qui agissent par procuration pour un État, la diversité, la prolifération et la professionnalisation des cyber-attaquants est, elle aussi, conséquente, hybride et composite.

Face aux cyber-attaques de tout ordre, la France avec l'ANSSI (Agence nationale de la sécurité des systèmes d'information) délivre pour tous les types d'acteurs des recommandations, accompagne les victimes de cyber-attaques et protège les organismes des secteurs vitaux aux intérêts de la Nation.

De même, les assureurs, pleinement conscients du risque cyber, ont développé depuis plusieurs dizaines d'années, d'abord aux États-Unis et au Royaume-Uni, puis en France, des polices de cyber-assurance. Plus mature outre-Atlantique, le marché de la cyber-assurance est alimenté par les grandes agences de notation qui incluent dans leur notation le risque cyber.

[1] Allianz risk barometer, janvier 2020

Cependant, on le remarque, le marché et les offres de cyber-assurance dans l'hexagone demeurent parfois l'apanage d'assureurs extra-européens. Si les grands groupes sont au fait des risques cyber, les entreprises plus modestes et les collectivités territoriales demeurent bien souvent démunies tant techniquement que juridiquement face aux cyber-agressions. De même, alors que la demande de cyber-assurance augmente, on note une rétractation de l'offre.

Dès lors comment faire gagner en maturité le marché de la cyber-assurance ? Comment mieux sensibiliser les petits organismes ? Comment réduire les réserves des assureurs ? Comment bien anticiper l'augmentation des cyber-sinistres ? Comment situer les assureurs dans le dispositif français de cybersécurité ? C'est à ces questions que vise à répondre le présent rapport.

Mot de Monsieur Guillaume Poupard, Directeur général de l'ANSSI (Agence nationale de la sécurité des systèmes d'information)

L'explosion de la cybercriminalité depuis 2019, avec une croissance extrêmement forte à la fois du volume de cyberattaques et du montant des rançons, a mis en lumière un écosystème cybercriminel professionnalisé et structuré. Alors que les cyberattaques par rançongiciel ont été multipliées par 4 entre 2019 et 2020, et que cette trajectoire se confirme depuis le début de l'année 2021 (+60%), leur impact économique et social est majeur. En effet, les victimes de telles cyberattaques sont souvent démunies et subissent des effets durables, notamment sur les plans financier et réputationnel. Face à cette situation, l'assurance cyber doit pouvoir jouer un rôle positif à la fois dans le déploiement de mesures de prévention et l'accompagnement des victimes en cas de cyberattaques pour les orienter et leur fournir une partie des outils nécessaires. Elle ne peut pas cependant contribuer à alimenter les activités cybercriminelles en systématisant le paiement des rançons.

De fait, la professionnalisation et la sophistication croissante des groupes de cybercriminels est directement liée à la rentabilité de leurs modèles économiques. Cette rentabilité est évidemment renforcée lorsque leurs cibles bénéficient d'assurances cyber qui prennent en compte le paiement des rançons. Les cybercriminels en ont pleinement conscience : ils ciblent désormais les fichiers des assureurs pour ensuite s'en prendre à leurs clients et avoir ainsi des garanties accrues de paiement. Il est donc indispensable d'enrayer la perception de rentabilité des cyberattaques par rançongiciels et le sentiment d'impunité des attaquants. Pour ce faire, l'interdiction ou a minima un encadrement strict de la couverture du versement des rançons dans les polices d'assurance cyber semble désormais indispensable pour placer l'ensemble des assureurs sur un pied d'égalité, tout en asséchant considérablement la manne financière des cybercriminels.

A contrario, les assurances peuvent jouer un rôle essentiel dans la prise en compte du risque cyber par les entreprises. Les assurances jouent en effet un rôle de tiers de confiance vis-à-vis de leurs assurés et leur donnent des outils de prévention pour faire face aux risques auxquels ils sont exposés. Elles ont également un pouvoir incitatif qui poussent leurs assurés à s'astreindre aux bonnes pratiques de cybersécurité, voire à réaliser des audits réguliers pour évaluer leur niveau de maturité. De même, lors de cyberattaques ou d'incidents de cybersécurité, les assurances peuvent permettre de limiter le préjudice, financier, moral et numérique, en offrant des assistances de qualité, à même d'aider la victime à faire face efficacement. La création de ce cercle vertueux indispensable mobilise pleinement le secteur assurantiel, qui s'investit directement dans l'assistance aux victimes. Je veux souligner à ce titre la participation remarquable de la Fédération française de l'assurance (FFA) ainsi que d'assureurs particuliers au dispositif cybermalveillance.gouv.fr.

Positionner les assureurs comme vecteurs d'une meilleure cybersécurité est une étape essentielle dans la construction d'un modèle durable de cybersécurité, alliant accompagnement et responsabilisation des acteurs privés.

Propositions

I) Clarifier et définir le droit relatif aux cyber-risques et cyber-attaques

1) Adopter une définition commune du cyber-risque et de la cyber-attaque ;
2) Clarifier la législation en matière de paiement des rançongiciels ;
3) Préciser la législation relative au paiement des amendes administratives ;
4) Subordonner l'activation des garanties assurancielles au dépôt de plainte à la suite d'une cyber-attaque.

II) Renforcer la résilience et la défense face aux cyber-risques

5) Promouvoir le dispositif cybermalveillance.gouv.fr auprès des entreprises et des collectivités ;
6) Créer un recueil anonyme des cyber-attaques frappant les entreprises géré par le GIP ACYMA (Cybermalveillance.gouv.fr);
7) Renforcer les moyens humains, matériels et financiers du GIP ACYMA ;
8) Inciter les institutions européennes à instaurer un « small business act » de la cybersécurité en France et favoriser dans la commande publique des solutions souveraines ;
9) Allonger la formation des magistrats en matière de cybersécurité ;
10) Augmenter les moyens humains, financiers et matériels des services de la justice, de la police et de la gendarmerie chargés de la lutte contre la cyber-criminalité ;
11) Sensibiliser au moins une fois par an les salariés des petites et moyennes entreprises aux risques cyber ;
12) Créer pour les collectivités, les administrations et les entreprises un prérequis en matière de cybersécurité ;
13) Créer au sein de l'État une agence nationale dédiée à des opérations cyber-offensives dans le secteur économique et industriel ;
14) Orienter directement les aides publiques aux collectivités et aux entreprises pour effectuer un audit de cybersécurité et à se doter d'un dispositif de cybersécurité ;
15) Imposer aux entreprises qui travaillent pour et/ou avec l'État et/ou des OIV /OSE à se doter d'une police d'assurance cyber ;
16) Développer un écosystème en rapprochant les assurances françaises des entreprises de cybersécurité françaises.

III) Développer le marché de la cyber-assurance

17) Inciter à la création en Europe d'un mécanisme d'évaluation des offres de cyber-assurance ;
18) Harmoniser à l'échelle française puis européenne les critères d'analyse des cyber-risques entre les assureurs ;
19) Créer une nouvelle branche d'assurance dédiée à la cyber-assurance ;
20) Développer des solutions hybrides de cybersécurité et de cyber-assurance pour les petites et moyennes entreprises et les collectivités.

I) Une effectivité juridique à garantir

Le constat est sans appel, pour une meilleure compétitivité et pour un meilleur service public, les entreprises et l'administration doivent se moderniser et accélérer leur passage au digital. Cependant, comme tout changement, la digitalisation n'est pas dépourvue de son lot de risques.

De plus, la crise sanitaire a joué un rôle d'accélérateur avec le recours massif au télétravail et la dématérialisation de nombreuses démarches et de nombreux échanges. Les cyber-criminels se sont, eux aussi saisis de cette opportunité pour multiplier les cyber-attaques.

Ces dernières ont mis en évidence la vulnérabilité des entreprises françaises, des collectivités territoriales, des administrations et des établissements publics face à ce phénomène de grande ampleur.

L'ANSSI (Agence nationale de la sécurité des systèmes d'information) estime que le nombre d'attaques a quadruplé depuis le début de la pandémie de Covid-19[2], et dénombre en 2020 une hausse de 225% des signalements d'attaques par rançongiciels par rapport à 2019[3].

De même, les tentatives de *phishing* ont augmenté de 400% (mars 2020-février 2021). Des opérations invasives qui augmentent de 80% le risque de défaillances des entreprises dans les trois mois qui suivent l'incident. Le nombre d'attaques de rançongiciels a par ailleurs été multiplié par quatre en un an. 192 attaques ont été répertoriées en 2020, contre 54 sur toute l'année 2019, en France, toujours selon l'ANSSI.

Ces chiffres attestent de la vulnérabilité de nos entreprises qui ne sont aujourd'hui ni suffisamment conseillées, ni convenablement préparées à s'en prémunir. Assurément, le risque des cyber-attaques est croissant, et le risque de divulgation des risques l'est encore plus puisque 23% des attaques pourraient résulter d'information de tiers-partie.

De plus, les rançongiciels sont devenus la première menace pour l'activité en passant de la sixième à la première place chez les victimes en termes de logiciels d'attaque de 2019 à 2020.

1) Des définitions à clarifier

Avant de décrypter l'état contemporain des offres de cyber-assurance, il convient de fixer les termes du sujet. C'est pourquoi, on retiendra dans le présent rapport la définition de la cyber-attaque comme : un acte malveillant visant à altérer les systèmes d'information (logiciels, fichiers, ordinateurs, serveurs, téléphones mobiles…).

On dénombre à ce jour plusieurs formes de cyber-attaques. Les plus courantes sont l'hameçonnage (ou *phishing*) où le cyber-attaquant se fait passer pour une personne de confiance (Administration, banque…) pour tenter d'obtenir des données.

[2] https://www.ssi.gouv.fr/agence/missions/rapport-dactivite-2020/
[3] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf

Le « rançongiciel » (ou *ransomware*) lorsque l'attaque consiste à chiffrer des données (par exemple les contacts fournisseurs, clients, des fichiers confidentiels…), puis le cyber-attaquant propose une clé de déchiffrement contre le paiement d'une rançon.

L'attaque par déni de service ou déni d'accès qui vise à bloquer l'activité de la cible, par exemple en rendant inaccessible un logiciel, le site internet par une congestion de flux.

Le sabotage qui vise à détruire tout ou partie des systèmes informatiques de la cible.

Et l'espionnage « par point d'eau » (ou *watering hole*) ou « par hameçonnage ciblé » (ou *spear phishing*) consistant à récupérer des données de la cible sans que celle-ci ne s'en rende compte.

Le kaléidoscope des cyber-agressions montre que la donnée avec l'avènement du digital est devenue le cœur des cyber-attaques. Assurément, la maîtrise des données représente un enjeu de sécurité et de souveraineté pour les États, un enjeu démocratique pour les individus et une source de création de richesses pour les entreprises. De ce fait, la donnée est devenue stratégique et vecteur de valeurs.

Pour le risque cyber une multitude de définitions existent : la Matmut[4] le définit ainsi : le risque cyber est une atteinte à des systèmes électroniques et/ou informatiques, des données informatisées (personnelles, confidentielles ou d'exploitation) à la suite d'un acte malveillant, une erreur humaine, une panne ou un problème technique. L'objectif est de détourner ou voler des données personnelles et/ou confidentielles, de paralyser l'activité de l'entreprise ou extorquer des fonds.

Alors que Northbridge Assurance[5] opte pour la définition suivante : les risques cyber sont les risques de perte financière, d'interruption des activités ou d'atteinte à la réputation d'une entreprise en raison d'une défaillance des systèmes de technologies de l'information. Il peut s'agir d'une intrusion volontaire, involontaire ou liée aux technologies de l'information.

On propose de définir le risque cyber comme : un ensemble de risques liés à une utilisation malveillante des systèmes informatiques et des technologies de l'information des particuliers, des administrations ou des entreprises.

Cette ingérence dans système menaçant le bon fonctionnement de l'activité de la cible visée, et/ou la captation des données, une surveillance de ses activités ou encore une paralysie partielle ou totale de son activité. L'intrusion peut être volontaire, involontaire et liée aux technologies de l'information. Elle entraîne le plus souvent des pertes financières.

Proposition n°1
Adopter des définitions communes de la cyber-attaque et du cyber-risque

[4] https://www.matmut.fr/pro/assurance-activite/cyber-risques
[5] https://www.northbridgeassurance.ca/blog/qu-est-ce-qu-un-cyberrisque/

2) Des régimes à optimiser

A) La rançon

Dans sa définition courante, la rançon est la somme que l'on exige pour délivrer une personne qu'on tient captive. Ici, dans le cadre du cyber-espace, il est question de rançongiciel que l'ANSSI définit comme une technique d'attaque courante de la cyber-criminalité. Le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement[6].

D'un point de vue légal, réglementaire ou administratif (autorités de contrôle et de régulation), il n'existe pas aujourd'hui d'interdiction formelle pour les assureurs de couvrir ce type de rançon dans le cadre d'une police d'assurance cyber. Un débat d'interprétation est toutefois possible.

Le code pénal précise à l'article 421-2-2[7] que : « Constitue également un acte de terrorisme le fait de financer une entreprise terroriste en fournissant, en réunissant ou en gérant des fonds, des valeurs ou des biens quelconques ou en donnant des conseils à cette fin, dans l'intention de voir ces fonds, valeurs ou biens utilisés ou en sachant qu'ils sont destinés à être utilisés, en tout ou partie, en vue de commettre l'un quelconque des actes de terrorisme prévus au présent chapitre, indépendamment de la survenance éventuelle d'un tel acte » ; et au nom du respect des mesures prévues par le Code monétaire et financier (articles L561-2 et L562-5 du Code monétaire et financier[8]), et par les règlements européens portant des mesures restrictives pour la lutte contre le blanchiment des capitaux et le financement des activités terroristes.

Par ailleurs, le règlement des rançons s'effectue en cryptomonnaies, réglementées quant à la traçabilité des transactions et l'identification des personnes (physiques ou morales) prenant part à la transaction[9]. Eu égard des risques de financement et d'incitation au « crime organisé » par les assureurs, la légalité du financement de rançons est aujourd'hui remise en cause.

Ainsi, le Haut Comité Juridique de la Place Financière de Paris a été missionné début 2021 par le Ministère de l'Economie et des Finances pour élaborer un rapport contenant des recommandations sur le sujet de la légalité de l'assurabilité du paiement des rançons. La Fédération française de l'assurance (FFA), comme de nombreux acteurs (ACPR, Direction générale du Trésor, avocats, professeurs de Droit, magistrats) participent aux travaux de ce groupe.

Selon la Fédération française de l'assurance (FFA) le remboursement du paiement des rançons n'est pas interdit par le législateur français dans le respect des lois sur les sanctions et le financement du terrorisme, et indique que la liberté de concurrence permet à chaque acteur de se positionner quant à la délivrance de cette garantie.

---

[6] CERTFR-2020-CTI-001, État de la menace rançongiciel à l'encontre des entreprises et institutions, 29 janvier 2020

[7] https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006149845/

[8] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042498840

[9] https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000042645365/

En sus de la nécessaire clarification légale à réaliser, le paiement des rançons alimente la cyber-criminalité et rien ne garantit que la rançon payée soit un gage de retour à la situation initiale. Le paiement encourage même les cyber-criminels à récidiver et en incite d'autres à concevoir des cyber-attaques. Les données modifiées par une application et chiffrées dans le même temps par le rançongiciel sont bien souvent définitivement corrompues[10]. Cette prise en charge des rançons favorise de surcroît le développement d'un véritable écosystème opaque.

Par ailleurs, le Trésor américain, dans une directive d'octobre 2020, indique que des sanctions pourront être infligées aux entreprises qui paient une rançon à la suite d'une attaque au rançongiciel[11]. Or, l'augmentation des attaques en France en 2020 est interprétée par certains professionnels de la sphère cyber comme un report des criminels du « marché américain » vers le « marché français » où la couverture des rançons existe et dont ces criminels peuvent encore tirer profit.

De plus, il ne faut pas oublier la portée extraterritoriale du droit américain en matière économique[12], car les entreprises françaises peuvent être concernées par ces sanctions. Je rappelle que 14% des entreprises françaises ont fait l'objet d'une cyber-attaque avec une demande de rançon. Dans près de deux cas sur trois, les victimes se sont acquittées de la rançon. Ce qui fait de la France l'un des pays qui paye le plus au monde ces demandes de rançons.

De même, selon l'assureur Hiscox, parmi les attaques les plus fréquentes figurent les rançongiciels avec une entreprise sur six qui a connu un incident de ce type en 2020 en France. L'assureur rappelle pareillement que 65 % des sinistrés en France admettent avoir payé une rançon[13].

Les collectivités locales et territoriales sont, elles aussi concernées. Lors d'une audition au Sénat sur la cybersécurité des ETI et des PME, le 15 avril dernier, Johanna Brousse, la vice-procureure chargée de la section « cybercriminalité » du parquet de Paris et Guillaume Poupard, le directeur général de l'ANSSI, ont pointé le rôle de certains assureurs dans le paiement de ces rançons[14]. Certains assureurs admettent, en effet, que le paiement de la rançon en dernier ressort fait partie de la promesse d'assistance que l'on peut faire et que le non-paiement d'une rançon n'est pas contractuellement écrit.

Pour toutes ces raisons, il convient d'inscrire dans la loi l'interdiction pour les assureurs de garantir, couvrir ou d'indemniser la rançon et se porter davantage vers la prévention, l'accompagnement et l'assurance des conséquences pour une entreprise.

---

[10] Attaques par rançongiciels, tous concernés comment les anticiper et réagir en cas d'incident ?, ANSSI, août 2020

[11] https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001

[12] Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale, Rapport à la demande de M. Edouard Philippe, Premier ministre, établi par M. Raphael Gauvain, Député de Saône-et-Loire, Mme Claire D'Urso, Inspectrice de la Justice, M. Alain Damais, Inspecteur des Finances et Mme Samira Jemai, collaboratrice au Groupe LaREM de l'Assemblée nationale, 26 juin 2019

[13] Rapport Hiscox 2021 sur la gestion des cyber-risques

[14] Délégation aux entreprises, Table ronde sur « La cybersécurité des ETI-PME-TPE : la réponse des pouvoirs publics », jeudi 15 avril 2021

De même à l'instar de nos collègues américains, il convient de sanctionner les entreprises, administrations ou collectivités qui procèdent au paiement des rançons à l'aide d'un tiers ou de manière direct.

Proposition n°2
Clarifier la législation en matière de paiement des rançongiciels

B) L'amende administrative

Au cours des dernières années, le législateur a accru les règles pesant sur les entreprises dans de multiples domaines visant la protection des données ou la lutte contre la corruption.

Ainsi, qu'il s'agisse de la création de nouvelles autorités régulatrices (telle que l'AFA, l'Agence française anticorruption) ou bien du renforcement des pouvoirs d'investigation ou de sanction d'autorités existantes (telle que la CNIL), la question de l'assurabilité des amendes administratives s'est, de cette façon, retrouvée au cœur de nombreux débats juridiques pour déterminer la légalité de ce type de couverture qui n'a fait, à ce jour, l'objet d'aucune interdiction formelle, ni de la part du législateur, ni de la part des autorités de contrôle.

C'est pourquoi, le Règlement Général sur la Protection des données (RGPD)[15] applicable dans le droit interne européen depuis le 25 mai 2018, a pour vocation de défendre les intérêts et les données personnelles du consommateur, ceci en lui accordant des droits plus larges que ceux énoncés dans la directive de 1995 (portabilité des données, droit spécifique pour les mineurs, instauration d'actions collectives, l'indemnisation de dommages matériel ou moral).

Cette règlementation européenne fait également référence à l'affaire Snowden de 2013 et vise à ce que les acteurs économiques fassent preuve davantage de transparence et d'une responsabilité accrue quant à la gestion des données.

Ainsi, les professionnels dès lors qu'ils traitent des données personnelles se doivent de mettre en place les outils de conformité comme un registre des traitements mis en œuvre, une notification de failles de sécurité, la certification de traitements, l'adhésion à des codes de conduites, la présence d'un délégué à la protection des données et la conduite d'analyses d'impact à propos de la protection des données.

En France, en cas de manquement, la CNIL (Commission nationale de l'informatique et des libertés) peut sanctionner l'entreprise concernée de différentes manières, notamment en prononçant une amende administrative pouvant s'élever jusqu'à 20 millions d'euros ou à hauteur de 4% du chiffre d'affaires monde de ladite entreprise.

Cette nouvelle règlementation incite les acteurs de l'assurance à adapter leurs produits, afin de mieux couvrir les conséquences pour les collectivités et les entreprises. Là encore deux thèses existent quant à l'assurabilité des amendes administratives.

[15] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/

Pour défendre la légalité de l'assurabilité des amendes administratives, les arguments résultent de l'article L. 113-1 du code des assurances[16] notant que la responsabilité de l'assuré reste techniquement assurable dès lors qu'elle est issue, soit d'une faute non intentionnelle, soit d'une faute intentionnelle commise par une autre personne dont l'assuré peut être tenu pour responsable.

L'article L. 121-2 du même code[17] prévoit d'ailleurs que l'assureur est garant des pertes et dommages causés par des personnes dont l'assuré est civilement responsable « quelles que soient la nature et la gravité des fautes de ces personnes ».

De surcroit, l'application d'une franchise vient maintenir une certaine moralisation des comportements des assurés concernés. Ainsi, dès lors que l'amende administrative résulterait d'une faute non intentionnelle de l'assuré, ou qu'elle serait intentionnelle, mais commise par une autre personne dont l'assuré est responsable (par ex. un dirigeant vis-à-vis d'employés), elle pourrait être couverte par un contrat d'assurance.

Par ailleurs, l'article 6 du code civil[18] prévoit qu'on « ne peut déroger par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs » et l'article 1162 du Code civil[19] prévoit également que « le contrat ne peut déroger à l'ordre public ni par ses stipulations, ni par son but, que ce dernier ait été connu ou non par toutes les parties».

Ainsi, contrairement à une dette de responsabilité civile, soumise au principe indemnitaire, une dette d'amende administrative n'a pas pour objet de réparer un préjudice, mais bien de sanctionner un comportement fautif ayant troublé un ordre public. À ce titre, elle ne serait donc pas assurable.

Face à cette tension juridique et au silence en creux des textes, sources d'insécurité juridique, les acteurs du secteur auditionnés demandent une position claire des autorités publiques.

Ainsi, on recommande l'autorisation de couverture et de prise en charge des amendes administratives par l'assureur.

Par ailleurs, les propos tenus lors des auditions ont démontré un défaut de recours à un dépôt de plainte de la part des victimes de cyber-attaques. Or, la plainte est l'étape préalable à l'ouverture d'une enquête judiciaire, et toute personne physique ou morale, ou organisation victime d'une cyber-agression, peut déposer plainte, et ce, que le cyber-attaquants soit identifié ou non. Une plainte déposée entraîne dès lors l'ouverture d'une enquête qui, elle-même, permet la préservation des preuves, le recours à des prestataires et à des experts techniques par les enquêteurs, le déploiement d'une coopération entre les services dédiés en France et avec leurs interlocuteurs étrangers.

Plus globalement, il convient d'inscrire dans le code des assurances la subordination de l'activation des garanties de cyber-assurance à un dépôt de plainte auprès des services compétents.

[16] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006791984/
[17] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032042697
[18] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006419285/
[19] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032041158

Propositions n° 3 et 4
Préciser la législation relative au paiement des amendes administratives
Subordonner l'activation des garanties assurancielles au dépôt de plainte à la suite d'une cyber-attaque

II) Une résilience à encourager

1) Un écosystème à renforcer

L'écosystème français de cybersécurité est très éclaté. D'une part, il y a les nombreux services de l'État dédiés, d'autre part de nombreuses entreprises intervenantes dans les différents domaines de la cybersécurité, du service au conseil en passant par la formation, l'audit et le soutien technique.

S'agissant des services étatiques, en matière de lutte contre la cyber-criminalité l'organisme Cybermalveillance.gouv.fr est l'interlocuteur de référence qui a dénombré une hausse de 155% de fréquentations de son site en 2020 et qui a accompagné pas moins de 10 000 entreprises[20].

Lancée début 2017 par l'ANSSI et le ministère de l'Intérieur, la plate-forme nationale d'assistance Cybermalveillance.gouv.fr, dirigée par M. Jérôme Notin, est un groupement d'intérêt public ACYMA (GIP ACYMA) qui accompagne les victimes de cyber-attaques avec une assistance en ligne et une mise en relation avec des experts en cyber-sécurité, sensibilise les usagers du cyber-espace aux problématiques de cyber-sécurité et observe l'évolution des cyber-menaces. Un dispositif de référence pour les entreprises et les collectivités territoriales est implanté dans tous les territoires.

En outre, le GIP ACYMA, membre du futur Campus Cyber, finalise actuellement la mise en place opérationnelle d'un Observatoire national de la menace et du risque numérique, pour lequel il convient d'augmenter le soutien de l'État.

De plus, au sein de la gendarmerie, on note le centre de lutte contre les criminalités numériques (C3N), qui est chargé de piloter la lutte contre la cyber-criminalité.

Au sein de la police judiciaire du ministère de l'Intérieur, se déploie une sous-direction en charge de la lutte contre la cyber-criminalité (SDLC). Au sein de préfecture de police de Paris, se mobilise une unité de police judiciaire spécialisée dans la lutte contre la cyber-criminalité, la Brigade de lutte contre la cyber-criminalité (BL2C).

Au sein du Ministère de l'Économie et des Finances, sont engagés la cellule Cyber douane de la direction nationale du renseignement et des enquêtes douanières (DNRED), le service de traitement du renseignement et d'action contre les circuits financiers (Tracfin) et le service national des enquêtes (SNE) de la direction générale de la concurrence, de la consommation et de la répression des fraudes du ministère de l'Économie qui peut être amenée à enquêter sur des affaires relatives à la cyber-criminalité.

[20] https://www.cybermalveillance.gouv.fr/medias/2021/04/Rapport-activite-cybermalveillancegouvfr-2020.pdf

Aussi, en février 2021 la gendarmerie a, au niveau opérationnel, lancé le commandement de la gendarmerie dans le cyber-espace (ComCyberGend) afin de mieux lutter contre la cyber-criminalité en regroupant dans ce nouveau commandement opérationnel depuis août 2021 toutes les composantes dédiées au numérique de la gendarmerie.

Sous l'autorité du directeur général de la Gendarmerie, lui-même sous la tutelle du ministère de l'Intérieur, cette nouvelle institution s'appuie sur 7 000 cyber-enquêteurs avec l'objectif d'une augmentation à 10 000 des effectifs, répartis dans onze antennes en région et trois principaux centres. S'adaptant à la configuration de la menace, l'effort du ComCyberGend est porté sur les rançongiciels.

Selon la gendarmerie nationale, plus de 101 000 procédures relatives au rançongiciel ont été ouvertes en 2020, soit plus 21% par rapport à 2019. La gendarmerie rappelle à ce titre qu'il y a eu seulement un dépôt de plainte pour 267 cyber-attaques. Preuve du phénomène des rançongiciels, selon la gendarmerie, 46% des victimes de rançongiciels sont des PME, 21% des TPE, 14% des administrations, et 9% des grands groupes[21].

Par ailleurs, présidé par M. Michel Van Berghe, depuis juillet 2019, le Campus cyber de la Défense est en cours de finalisation. Celui-ci vise à rassembler en un même lieu des acteurs de la cybersécurité privés, publics, et de toutes tailles. Ainsi, on retrouvera les services de l'État chargés de la cybersécurité, des grands groupes, des jeunes entreprises, des instituts de formation et des associations. Le but est de fédérer l'ensemble des acteurs de la cybersécurité sur le sol français afin de créer des synergies entre eux par la réalisation de projets communs. L'administration du Campus est réalisée par une SAS détenue à 51 % par le secteur privé et 49 % par le secteur public. Ainsi, une coordination avec l'industrie de l'assurance, vecteur de prévention serait la bienvenue.

Propositions n°5, 6 et 7

Promouvoir le dispositif cybermalveillance.gouv.fr auprès des entreprises et des collectivités

Créer un recueil anonyme des cyber-attaques frappant les entreprises gérées par le GIP ACYMA (Cybermalveillance.gouv.fr)

Renforcer les moyens humains, matériels et financiers du GIP ACYMA

Enfin, au ministère de la Justice, le procureur de la République, le pôle de l'instruction, le tribunal correctionnel et la cour d'assises de Paris disposent d'une compétence concurrente nationale sur les cyber-attaques.

En effet, ils sont chargés des atteintes aux systèmes de traitement automatisé de données (STAD) et des atteintes aux intérêts fondamentaux de la Nation, dont il n'est pas interdit de prévoir qu'à l'avenir des cyber-attaques pourront porter atteinte, comme le rappelle le Club des juristes dans un rapport. La juridiction nationale dédiée à la lutte contre la criminalité organisée (JUNALCO) est confiée au parquet à la section J3.

Lors des auditions, d'aucuns ont pointé le manque de lisibilité dans la cohérence d'ensemble de tous ces services chargés de lutter contre la cyber-criminalité.

[21] https://www.latribune.fr/technos-medias/internet/la-gendarmerie-nationale-en-premiere-ligne-contre-les-cybercriminels-891778.html

De même, les auditions montrent que les services judiciaires sont dénués de moyens suffisants pour mener à bien leurs différentes enquêtes, de surcroit face à des cyber-attaquants de plus en plus structurés.

En réalité, le parquet dédié ne compte que trois magistrats face à des dossiers toujours plus nombreux et complexes, suivant un Code pénal qui n'est pas assez en phase à la lutte contre la cyber-criminalité, avec des difficultés liées à l'obtention et à la validité des preuves numériques et un manque de ressources humaines et matérielles pour suivre les flux de monnaies virtuelles qui servent dans la plupart des situations à payer les rançons.

Du civil au militaire, en passant par la police, la gendarmerie et la justice, **il convient de renforcer la formation en cyber-sécurité.** En effet, sans augmentation significative des compétences et du nombre de personnes formées, nous ne pourrions agir efficacement pour la résilience et lutter contre la criminalité dans le cyber-espace.

Propositions n°9 et 10
Allonger la formation des magistrats en matière de cybersécurité
Augmenter les moyens humains, financiers et matériels des services de la justice, de la police et de la gendarmerie chargés de la lutte contre la cyber-criminalité

S'agissant de l'ANSSI, celle-ci pilote la stratégie de la France en matière de défense et de sécurité des systèmes d'information. Dévoilée en 2013, elle vise le renforcement de la cybersécurité des infrastructures nationales dites vitales. Concrètement, la cybersécurité est supervisée par un réseau de CERT (Computer Emergency Response Team) déployés par l'ANSSI.

Cette compétence générale de l'ANSSI sur les grandes entreprises et sur les infrastructures et réseaux vitaux du pays est d'ailleurs consacrée dans la loi de programmation militaire de 2013[22]. Depuis, l'ANSSI peut imposer aux organismes d'importance vitale la mise en place de dispositifs de cybersécurité. Toutefois, si la tendance va dans un sens positif, selon le cabinet Wavestone, utilisant le référentiel NIST, seulement 48% des entreprises françaises collaborant avec ce cabinet, essentiellement des grandes entreprises, sont matures sur le plan de la cybersécurité.

De même, on relève globalement que les dispositifs étatiques ne couvrent pas suffisamment les TPE/PME, ce qui fait de celles-ci des cibles pour les cyber-attaquants. Or, de cette cyber-sécurisation des entreprises dépendent l'emploi et de la pérennité de l'économie en France.

Plus spécifiquement, l'ANSSI traite en particulier de la cybersécurité des OIV et OSE. Les OIV (Opérateurs d'importance Vitale) recouvrent un statut inscrit dans le cadre du dispositif interministériel de sécurité des activités d'importance vitale (SAIV), lui-même inscrit dans le Code de la Défense nationale. Concrètement, certains acteurs, publics ou privés, gèrent des équipements et des installations indispensables au fonctionnement de la Nation, donc à sa survie.

[22] https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000028338907

Cette classification a été inscrite par la loi de programmation militaire de 2013[23], même si pour des raisons de sécurité évidente, la liste des OIV est confidentielle. Les OSE (Opérateurs de services essentiels) se situent dans la même logique de protection. Ce statut découle de la directive européenne NIS qui élargit le dispositif dédié aux OIV à des acteurs dont les interruptions répétées ou de longue durée peuvent avoir des effets négatifs sur le fonctionnement du pays. La liste des OSE est publiée par décret au Journal officiel. Les estimations se situent autour de 600 OIV et OSE confondus actuellement.

Enfin, si la cyber protection d'une partie du monde économique français est assurée par l'ANSSI, la cyberdéfense en la matière est une grande absente.

Pour rappel, le Commandement de la cyberdéfense (COMCYBER) des armées est limité à des finalités d'intérêts militaires.

Ainsi, il convient de créer un pôle dédié aux opérations de cyberdéfense économique de manière offensive afin d'assurer la défense des intérêts économique de la France.

Proposition n°13
Créer au sein de l'État une agence nationale dédiée à des opérations cyber-offensives dans le secteur économique et industriel

Le secteur privé de la cybersécurité française est un formidable atout. Les entreprises sont nombreuses et de grande qualité. Cette industrie en France réalise annuellement environ 13 milliards d'euros de chiffre d'affaires et emploie strictement dans la cybersécurité environ 70 000 personnes.

La filière française de la cybersécurité est non seulement très exportatrice avec 4,4 milliards de chiffre d'affaires à l'exportation, mais elle est en forte croissance avec un taux de valeur ajoutée de 43% selon l'Observatoire de l'Alliance de la confiance numérique en 2021. Toujours selon l'ACN, on dénombre un peu plus de 2000 entreprises dans le domaine de la cybersécurité, dont 65 grandes entreprises, 75 entreprises de taille intermédiaire, 636 PME et 1 355 micro-entreprises.

L'offre en matière de cybersécurité est de ce fait assez disparate puisque 63 % de ces entreprises comptabilisées par l'ACN réalisent moins de 2 millions d'euros de chiffre d'affaires par an[24].

Fort de ces chiffres, la France dispose avec ses entreprises de cybersécurité des meilleurs outils de cyber-protection après les États-Unis, Israël et la Grande-Bretagne, avec des domaines dans lesquels elle excelle comme le *deep learning*, la cryptographie, la *blockchain* et l'informatique quantique. Or, il convient de passer d'un écosystème de la cybersécurité en soi à un écosystème pour soi, de fédérer toutes ces entreprises et d'accorder davantage nos ambitions et nos moyens en matière de souveraineté numérique en favorisant l'achat par les collectivités et les administrations de solutions souveraines.

[23] https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000028338907
[24] Observatoire ACN 2021 de la Confiance Numérique

Cependant, le secteur fait face à certaines difficultés : un manque de coordination permettant une offre de service globale, manque de main d'œuvre et enfin la difficulté d'accéder à la certification de l'ANSSI. En effet, le déficit de ressources humaines dans le secteur de la cybersécurité est un phénomène mondial que l'on observe avant le début de la crise sanitaire, et mécaniquement, ce sont les structures entrepreneuriales les plus modestes qui en pâtissent le plus. Ainsi, selon le rapport Global Knowledge de novembre 2020 sur les compétences et les salaires IT, 45 % des entreprises considéraient que le déficit de compétences dans ce domaine s'est accru au cours des dernières années.

Outre le manque de personnels dans ce domaine, on constate des compétences très variables d'un expert à l'autre. Ainsi, près de 78 % des décideurs informatiques mondiaux font face à des lacunes critiques en matière de compétences[25]. Plus spécifiquement dans l'hexagone, Pôle Emploi dénombrait 775 577 salariés dans le secteur numérique, dont 58 % dans l'informatique et estime que 191 000 postes seront à pourvoir d'ici à 2022. Entre des préjugés qui ternissent l'image des professionnels en cybersécurité, des évolutions de carrière pas suffisamment connues dans ce domaine, et une concurrence forte, la situation de pénurie semble s'ankyloser[26].

Ainsi, il convient d'instaurer des certifications intermédiaires des solutions de cybersécurité permettant aux entreprises du secteur de travailler avec les TPE/PME/ETI, ainsi que les collectivités, ainsi que la collaboration étroite avec l'industrie de l'assurance, permettant le référencement des entreprises de la cybersécurité de confiance.

Proposition n°8 et 16
Inciter les institutions européennes à instaurer un « small business act » de la cybersécurité et développer un écosystème en rapprochant les assurances françaises des entreprises de cybersécurité

2) <u>Des acteurs à sensibiliser</u>

Une étude datant du printemps 2021, soit plus d'un an après le début de la crise sanitaire, montre que neuf entreprises sur dix estiment qu'il est nécessaire de se prémunir contre les cyber-attaques, une sur trois n'utilise toujours pas d'antivirus. De même, toujours selon cette même enquête, le budget dédié à la cybersécurité n'excède pas le stade des 1 000 euros par an pour six entreprises françaises sur dix[27].

Par conséquent, le tissu économique français, comme les administrations et les collectivités territoriales ont effectué ces deux dernières décennies une digitalisation de leurs différentes activités et de leur fonctionnement à « marche forcée ». L'une des conséquences de ce processus a été de minorer pour partie les investissements en termes de cybersécurité, que cela soit sur le plan de la sensibilisation des collaborateurs, de la mise en place de systèmes de cybersécurité dans les systèmes d'information ou de la couverture assurantielle des risques cyber.

[25] Rapport Global Knowledge 2020 sur les compétences et les salaires IT, Global Knowledge, 11 novembre 2020
[26] Les métiers du numérique : quelles opportunités d'emploi ?, Pôle Emploi, janvier 2020
[27] https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/global-data-protection-index-2020-snapshot.pdf

De même, 80% des entreprises admettent que le développement du numérique en leur sein a été plus rapide que sa sécurisation et en 2016, seulement 38 % des entreprises françaises estimaient que leur risque de subir une cyber-attaque était important ou très important. Or, la cyber-criminalité s'est professionnalisée et attaque après un processus de profilage et de ciblage.

En outre, selon une enquête menée par l'assureur Hiscox, le nombre d'entreprises visées par une cyber-attaque est passé entre 2019 et 2020 de 34 % à 49 % en France et si les entreprises françaises sont plus ciblées, celles-ci sont aussi parmi celles qui ont le moins fait augmenter leur budget en matière de cybersécurité avec une hausse de 15 % en moyenne en France contre +25 % au niveau mondial.

Toutefois, 51% des entreprises françaises se jugent plus vulnérables à une cyber-attaque depuis le début de la crise sanitaire. Toujours selon cet assureur, la proportion d'entreprises ayant souscrit un contrat d'assurance dédié aux cyber-risques a peu progressé en 2020 par rapport à 2019 : 27 % (+1%). Les TPE sont les moins susceptibles de souscrire un tel contrat (44 % n'en ont aucune intention).

Néanmoins, de plus en plus d'entreprises et de collectivités prennent conscience des risques cyber, parfois à la suite d'un grave sinistre. Cependant, elles ne savent pas toujours comment commencer, et à qui faire appel.

Il convient de rappeler que le risque cyber est le deuxième plus important auquel doivent faire face les organismes tant privés que publics selon l'assureur Allianz, et ce alors que selon IBM, le coût moyen mondial d'une cyber-attaque pour une entreprise se situait à environ 3,62 millions de dollars en 2017 contre 3,92 millions en 2019 et les violations de données, IBM estime que le coût pour les entreprises a augmenté de 12% sur les cinq dernières années[28].

De même, outre la perte financière directe en raison d'un arrêt d'activité, une cyber-attaque porte atteinte à l'image de l'entreprise auprès notamment des investisseurs, mais également des clients et de l'opinion publique. Elle porte également des risques légaux liés à une rupture contractuelle des engagements de la société et des pénalités pour non-respect de ceux-ci. Enfin, une cyber-agression fait peser un grand risque de perte de propriété intellectuelle et des données chez les sinistrés.

En sus des menaces sur la continuité de l'activité économique, l'on a pu le constater avec les cyber-attaques dont ont fait l'objet récemment des établissements de santé et des collectivités, que ce sont les services publics essentiels et vitaux qui peuvent être atteints.

Enfin, on rappelle qu'une entreprise ou une collectivité ne vit pas en vase clos dans le cyber-espace. Elle n'est véritablement protégée que si l'ensemble de son écosystème l'est également (fournisseurs, sous-traitants… etc.). Plusieurs exemples récents de cyber-attaques montrent que pour atteindre un grand groupe industriel ou financier relativement bien armé sur le plan de la cybersécurité, les cyber-criminels l'atteignaient en s'attaquant aux sous-traitants, moins protégés.

[28] https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years#assets_all

Proposition n°11, 12, 14 et 15

Sensibiliser au moins fois par an les salariés des petites et moyennes entreprises aux risques cyber

Créer pour les collectivités, les administrations et les entreprises un prérequis en matière de cybersécurité

Orienter directement les aides publiques aux collectivités et aux entreprises pour effectuer un audit de cybersécurité et à se doter d'un dispositif de cybersécurité

Imposer aux entreprises qui travaillent pour ou avec l'État ou des OIV /OSE à se doter d'une police d'assurance cyber

III) Une offre assurantielle à dynamiser

1) Un marché jugé insuffisant

Le marché de la cyber-assurance est apparu dans l'hexagone depuis une quinzaine d'années. En effet, les premières véritables initiatives des assureurs en France dans ce domaine datent de 2007, avec une structuration croissante des offres au cours des années 2010. Toutefois, ce marché reste timide et le taux de pénétration très faible malgré une augmentation des primes en assurance cyber de 49% entre 2019 et 2020, passant de 87 M€ à 130 M€ (AMRAE). Il faut interpréter cette augmentation avec prudence au regard des recommandations des autorités de contrôle prudentiel, ainsi qu'une forte évolution tarifaire à la hausse lors des renouvèlements des programmes. Le marché de cyber-assurance en France présente, clairement de nombreux handicapes et nécessite un effort de structuration.

A) Un marché de l'offre déséquilibré et concentré

Malgré un marché d'assurance très développé, structuré et encadré en France, les offres en cyber-assurance sont concentrées aux mains d'un petit nombre de porteurs de risques. En effet, les acteurs reconnus de la cyber-assurance viennent historiquement et essentiellement des États-Unis et de Grande-Bretagne, comme AIG, CHUBB, AXIS, Liberty Mutual, ou The Hartford. Dans un contexte d'hyper-compétition économique, on peut s'interroger sur la résilience des agents économiques français lorsque celle-ci dépend uniquement d'opérateurs extra-européens. De même si la plupart de ces assureurs ont des implantations sur le continent européen, la décision des souscriptions s'agissant des grands risques se trouvent bien souvent hors de l'Union européenne.

L'essentiel des cyber-assureurs des grands comptes sont peu nombreux et historiquement extra-européens. Or, il faut rappeler que le sujet de la cybersécurité est extrêmement sensible en matière d'accès à la structure et aux secrets des affaires de l'assuré. De plus, un marché sain est un marché ouvert et concurrentiel, ce sont ces conditions qui permettent l'évolution favorable de l'offre pour les clients.

Le ratio de sinistres à primes dégradé explique partiellement cette concentration. Toutefois, les auditions ont mis en évidence d'autres facteurs, certains traités précédemment : la relative « inassurabilité » des entreprises par défaut de prévention, le manque de données et de recule sur ce marché immature.

D'autres éléments révélés lors des auditions méritent un développement et des recommandations.

Ainsi, la frilosité du marché de l'assurance français est intimement lié à la rétractation des capacités du marché assurantiel et de réassurance. En effet, le marché de la réassurance est un marché mondial, ainsi les capacités allouées par les réassureurs à la France et au risque cyber sont faibles, voir en diminution. Ceci est une conséquence de l'augmentation dans le monde du nombre et de l'intensité des risques dit systémiques. Pour rappel le transfert de risque à l'assurance ne peut se faire qu'à condition que celui-ci soit non systémique et aléatoire.

Le marché de l'assurance souffre, quant à lui d'une part de la réglementation européenne complexe, dans le but de protéger du consommateur, mais qui est extrêmement exigeante en termes de solvabilité, donc limitante en termes de prise de risques. D'autre part, le marché de l'assurance européen manque d'organisation quant aux capacités financière. Le Brexit ayant rendu impossible l'accès à la bourse des capacités organisé par le Lloyd's Londres, les assureurs européens ne se sont pas suffisamment structurés malgré l'installation d'une filiale de Lloyd's à Bruxelles. En effet, depuis le début de l'année 2019, les nouvelles polices d'assurance directe non-vie de l'espace économique européen ont été souscrites par Lloyd's Europe et celles qui ont été renouvelées ont fait l'objet d'un transfert à Lloyd's Europe. La différence de maturité au sujet du cyber-risque entre l'Europe continentale et la Grande-Bretagne, ainsi que la complexité de coordonnées les porteurs de risque pénalise l'espace économique européen et ne permet pas de couvrir davantage d'agents économiques et de collectivités.

Il s'agit là de freins majeurs qui ne touchent pas uniquement le secteur des risques émergents, mais aussi d'autres typologies de risques, ce qui empêche le tissu économique français de concevoir leurs programmes de couverture assurantielle. L'une des réponses à la problématique des capacités est de rendre le régime français des captive d'assurance et de réassurance compétitif.

B) L'inégalité de couverture

Toujours d'après l'étude de l'AMRAE près de 87% des grands groupes bénéficient d'un programme d'assurance cyber, 8% d'ETI, 0,0026% des PME et 1% des collectivités. Ce manque de mutualisation entre les assurés a pour conséquence le déséquilibre financier évoqué précédemment.

De plus, le niveau de garanties est bien en deçà des besoins réels des assurés. En moyenne les grands groupes sont couverts à hauteur de 38M€ pour un chiffre d'affaires annuel de plus d'1,5 milliards d'euros. Pour les ETI la couverture moyennes est de 8M€, pour rappel il s'agit des entreprises au chiffre d'affaires variant de 50M€ à 1,5Milliard€. Le risque d'un effet ciseau est réel, puisque les primes et les franchises augmentent chaque année.

Le constat est sans appel, le niveau des capacités allouées au risque cyber pour chaque assuré est sous-dimensionnée et ne permet pas de le protéger convenablement. Plus globalement la cartographie des couvertures démontre que le tissu économique français, ainsi que les collectivités restent vulnérables, même quand ils s'assurent.

C) Point de vue des autorités

Les autorités, en France comme à l'échelle européenne, du contrôle prudentiel en ont pris conscience et ont élaboré plusieurs recommandations en matière d'appréhension du risque cyber.

Face à l'exposition croissante des acteurs individuels, privés et publics aux cyber-risques et par conséquent des assureurs, le régulateur français, l'ACPR, a, fin 2019 alerté le secteur sur le manque de structuration du marché de la cyber-assurance, la trop grande variété des offres de cyber-assurance et d'un manque de données sur les cyber-risques[29]. Ce constat pousse l'ACPR à encourager, la création au sein de l'Union européenne d'un mécanisme commun d'évaluation des offres de cyber-assurance et la standardisation des critères d'analyse des cyber-risques entre les assureurs, afin de créer une nouvelle branche d'assurance dédiée au cyber.

L'ACPR relève aussi une division des garanties en deux segments, d'une part, les garanties explicites qui sont clairement mentionnées dans les contrats, et d'autre part les garanties implicites où la couverture des risques cyber n'est pas expressément intégrée dans le contrat, une forme de garanties silencieuses.

L'ACPR notait dans les garanties implicites l'imprudence des assureurs et leur potentielle trop grande exposition, comme en témoigne l'explosion du ratio sinistres à primes, qui passe de 84% en 2019 à 167% en 2020[30].

Ainsi, le régulateur recommandait aux acteurs du secteur d'améliorer la connaissance de leur exposition et plus largement des cyber-risques, d'harmoniser la terminologie de la cyber-assurance, et de faire de l'assurance un vecteur de prévention en termes de cybersécurité.

Outre son avis sur le marché de la cyber-assurance en 2019, le régulateur français a publié en juin 2021 vingt-cinq recommandations afin de hausser le niveau de cybersécurité des assureurs eux-mêmes. En effet, non seulement le coût des cyber-sinistres augmente mais la menace de cyber-attaques augmente également sur toutes les entreprises, dont celles du secteur de l'assurance.

L'ACPR poursuit avec ces recommandations les propositions d'octobre 2020 du régulateur européen, l'EIOPA, visant à harmoniser en Europe les normes en matière de cybersécurité chez les assureurs.

L'EIOPA recommande, également d'améliorer la lisibilité des contrats de cyber-assurance tant pour les assurés que les assureurs, de veiller à faire de l'assurance un outil de prévention des cyber-risques, de mener un dialogue avec l'industrie de la cybersécurité, d'accumuler davantage de données relatives aux cyber-incidents, et d'établir des règles de base et un vocabulaire commun à l'échelle européen sur les offres de cyber-assurance.

[29] https://acpr.banque-france.fr/communique-de-presse/la-distribution-des-garanties-contre-les-risques-cyber-par-les-assureurs

[30] LUCY : LUmière sur la CYberassurance, AMRAE, Mai 2021

2) Des pistes d'évolution

A) Le cordonnier mieux chaussé

A l'instar du rapport commun des superviseurs européens de la finance (European supervisory authorities), à savoir l'Autorité bancaire européenne (EBA), celle des marchés financiers (Esma) et celle des assurances (Eiopa) sur les risques en septembre 2021, **il convient de monter les compétences des assureurs sur leur propre risque cyber, ainsi que sur l'exposition de leur portefeuille**.

Par ailleurs, le taux de pénétration ne s'améliorera pas sans une formation particulière des agents chargés de la distribution, qu'il s'agisse des réseaux salariés, des agents généraux ou de courtiers en assurance. En effet, parmi les risques pesant sur les institutions financières, l'ESA alerte sur le cyber-risque en mentionnant le triplement des cyber-attaques dans la décennie et rappelant qu'une cyber-agression contre une institution financière peut contaminer l'ensemble du système financier et ainsi causer de graves conséquences sur l'accès aux liquidités et d'instabilité sur les marchés financiers[31]. Enfin, l'ESA rappelle que les institutions financières sont des cibles de choix pour les cyber-criminels et recommande à celles-ci de hausser leur niveau de cybersécurité.

Propositions n°16
Inclure dans la formation des réseaux de distribution la connaissance du cyber-risque et le volet assurance cyber

B) L'offre

Afin de mieux couvrir le cyber-risque le marché européen des capacités doit mieux s'organiser. Aucun assureur n'étant capable de s'exposer en étant le seul porteur de risque, il est utile qu'il ait une coordination permettant aux assureurs européens de joindre leurs efforts afin de répondre aux besoins des entreprises européennes.

Par ailleurs, le bilan dressé par les régulateurs français et européens corrobore le constat fait lors des auditions sur la disparité et l'immaturité du marché de la cyber-assurance. En effet, il est indispensable que les acteurs du marché français se coordonnent afin d'harmoniser le vocabulaire, les offres et les critères de sélection du risque. Le CCSF, cellule de dialogue des acteurs du marché, peut être le lieu de travail approprié.

Propositions n°17 et 18
Inciter à la création en France et en Europe d'un mécanisme d'évaluation des offres de cyber-assurance
Harmoniser à l'échelle française puis européenne les critères d'analyse des cyber-risques entre les assureurs
Interroger le réassureur publique, CCR, sur ses capacités d'appréhender les risques émergeants
Envisager le partenariat public-privé pour le segment systémique du risque cyber

[31] Joint committee report on riks and vulnerabilities in the EU financial system, septembre 2021

Le développement de la connaissance du risque parait incontournable, les actuaires auditionnés m'ont fait part de leur difficulté à récolter, pondérer et analyser une masse significative d'informations relatives aux cyber-risques. Elle n'est toutefois pas essentielle à l'amélioration de l'offre, puisque le cyber-risque est en constante évolution.

De même, la couverture d'un risque exige une large connaissance de l'assuré ou du prospect par l'assureur afin de bien appréhender la nature des risques qui peuvent peser sur lui. A ce jour, le nombre d'experts et d'agence de notation en risque cyber en Europe est bien trop limité.

Afin d'harmoniser davantage l'assurance des cyber-risques, la notation des agents économiques en matière de cybersécurité est de plus en plus courante, d'abord aux États-Unis, et plus embryonnaire, mais certaine en Europe, notamment avec la seule agence française de cyber-notation Cyrating, crée en 2018.

Plus globalement, les principales agences de notation américaines ajoutent de plus en plus le risque cyber dans leur notation. Même si le risque cyber n'est pas le critère principal dans l'analyse des agences de notations, celles-ci intègrent de plus en plus dans leur appréciation la capacité des entreprises à résister à une cyber-attaque. Comme en témoigne le communiqué de l'agence Standards & Poors en 2015 informant que l'agence « pourrait émettre une révision à la baisse si une banque semblait mal préparée à faire face à une cyber-attaque ou à la suite d'une violation causant des dommages importants à la réputation d'une banque ou entraînant des pertes financières substantielles ou des dommages juridiques »[32]. Toutefois, le secteur de la cyber-notation étant essentiellement composés d'entreprises américaines (Bitsight, Security Score Card), une problématique subsiste en termes de souveraineté et de protection des données des actifs économiques français.

Enfin, interlocuteur privilégié des entreprises, l'assureur ou l'intermédiaire chargé du conseil doit élaborer un programme de prévention en matière de cyber-risque, ainsi que fédérer autour de soi un écosystème permettant une meilleure lisibilité, veillant au respect des prérequis en termes de cybersécurité de leurs différents clients. Une prévention indispensable à la compétitivité, à la solidité et à la résilience des entreprises. Selon un sondage pour le Club des experts de la sécurité de l'information et du numérique (CESIN) par OpinionWay, 75% des entreprises françaises sondées ne s'adressent pas à leur assureur lors d'une cyber-attaque[33]. De même, 73 % des dirigeants d'entreprises européennes n'auraient qu'une faible connaissance de la cyber-assurance et 50 % d'entre eux n'auraient pas connaissance de l'existence de garanties risques cyber en cas de fuites de données selon Lloyd's[34].

Propositions n°19 et 20

Créer une nouvelle branche d'assurance dédiée à la cyber-assurance

Développer des solutions hybrides de cybersécurité et de cyber-assurance pour les petites et moyennes entreprises et les collectivités

[32] Cyber Risk And Corporate Credit, Standard & Poors, 2015

[33] 6ème édition du baromètre annuel du CESIN, 2021

[34] Loyd's, Faire face aux menaces cyber, 2016

Conclusion

Les grands groupes se sont assurément saisis du risque cyber, en termes de prévention des entreprises de tailles plus modestes, des collectivités territoriales et des administrations, celle-ci est encore parcellaire et discontinue.

Prévention, acculturation et formation sont des étapes nécessaires, en sus de la souscription à une assurance cyber, pour se prévenir des cyber-attaques et de ses conséquences financières, juridiques et réputationnelles pour toute organisation.

En effet, on le constate régulièrement, la majorité des attaques par rançongiciels proviennent d'hameçonnage. Il convient donc d'acculturer l'ensemble des collaborateurs d'une société au risque cyber. Des campagnes de formations plus poussées et régulières doivent être déployées.

Dans ce cadre, l'industrie de l'assurance s'impose comme le vecteur indispensable de la prévention à destination des entités publiques comme privées, afin que l'ensemble gagne en résilience face à la cyber-menace.

De ce fait, outre la nécessaire prise de conscience et de l'adoption du comportement adéquat de la part des assurés, les assureurs doivent également déverrouiller les freins au développement en France d'un marché mature de la cyber-assurance.

La levée de ces réserves est un levier nécessaire à l'enclenchement d'un mouvement vertueux pour le fonctionnement de ce marché. Moins de rétractations chez les assureurs et plus de données partagées par les assurées. Plus d'informations pour mieux cartographier les risques et ainsi, plus d'offres de cyber-assurance adaptées.

Aussi, afin de sécuriser les acteurs de la cyber-assurance, il est nécessaire de clarifier le cadre juridique, et le circuit de lutte contre les rançongiciels par des mécanismes d'interdictions, d'amendes et de plaintes.

De même, c'est tout un écosystème de la cyber-assurance qu'il convient d'encourager en rapprochant les assurances des entreprises de cybersécurité et ce, avec le concours de l'État. En réalité, la cyber-assurance doit être partie prenante de la stratégie française de la cybersécurité annoncée par le Président de la République Emmanuel Macron au printemps dernier, comme du volet transition numérique du plan France Relance.

Annexes

Les prérequis non-exhaustifs de l'hygiène numérique :

- Choisir avec soin et renouveler régulièrement ses mots de passe ;
- Connaitre les utilisateurs de son système d'information et ses prestataires ;
- Effectuer régulièrement des sauvegardes ;
- Supprimer systématiquement tous les éléments d'authentification (identifiants, mots de passe) définis par défaut sur les équipements (imprimantes, serveurs, box…) ;
- Ne jamais conserver les mots de passe dans des fichiers ;
- Ne pas préenregistrer les mots de passe dans les navigateurs ;
- Exiger une double authentification pour les actions d'administration ;
- Réservez et délimiter l'accès et l'utilisation au service informatique et identifiez précisément les différents utilisateurs du système et les accès qui leur sont accordés (dirigeants, salariés, alternants, stagiaires…) ;
- Ne pas utiliser les connexions Wi-Fi publics ;
- Modifiez la clé de connexion par défaut des box par un mot de passe ;
- Activer la fonction pare-feu de la box
- N'installez uniquement des applications nécessaires et contrôler les accès autorisés à ces applications ;
- Ne pas ouvrir les pièces jointes envoyées par des destinataires inconnus
- Ne jamais répondre par courriel à une demande d'informations confidentielles
- Désactivez l'ouverture automatique des documents téléchargés sans analyse antivirus préalable ;
- Ne pas héberger de données professionnels sur ses appareils personnels et inversement ;
- Former régulièrement les administrateurs des systèmes d'information ;
- Utiliser des produits et travailler avec des entreprises agrées par l'ANSSI ;
- Conférer le poste d'administration la capacité de bloquer l'accès à internet ;
- Chiffrer les périphériques de stockage ;
- Former régulièrement les personnels dédiés à la sécurité des systèmes d'information ;
- Sensibiliser continuellement les utilisateurs aux bonnes pratiques d'hygiène numérique ;
- Se doter d'un inventaire à jour et exhaustif des droits d'accès des utilisateurs ;
- Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs
- Autoriser la connexion au réseau aux seuls équipements connus ;
- Identifier nommément tous les utilisateur d'un réseau ;
- Chiffrer les informations confidentielles transmises au moyen d'internet ;
- Contrôler et sécuriser l'accès aux salles serveurs et aux locaux informatiques ;
- Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information ;
- Utiliser un réseau dédié et cloisonné pour l'administration du système d'information ;
- Réaliser des contrôles et audits de sécurité réguliers ;
- Désigner clairement auprès du personnel un référent en sécurité des systèmes d'information
- Définir une procédure de gestion de crise cyber.

La cyber-taxonomie de l'assurance :
Afin de mieux prendre en compte le risque cyber, qui se joue des frontières étatiques, l'EIOPA (Autorité européenne des assurances et des pensions professionnelles) entend promouvoir le développement d'un système harmonisé d'assurance des risques et l'élaboration d'une taxonomie harmonisée pour la déclaration des cyber-incidents afin d'étayer le modèle de la cyber-souscription, à l'aide d'une base de données centralisée (anonymisée) sur les cyber-incidents[35].

En effet, eu égard à la grande diversité des libellés de police existant sur le marché, il convient selon l'autorité européenne d'améliorer la compréhension commune et cohérente de la terminologie et des définitions de la cyber-assurance.

La complexité actuelle due à la vaste gamme de libellés de polices différents, au manque d'information, à l'absence d'un système de gestion des risques, de différentes formulations de polices et l'absence de définitions et d'exclusions communes entraîne des difficultés de compréhension pour les clients, les courtiers et les assureurs.

Ainsi, l'assurance a formalisé sa propre cyber-taxonomie comme le coût de l'atteinte à la vie privée où tous les frais, coûts, dépenses et honoraires raisonnables et nécessaires encourus par l'assuré pour retenir les services d'un comptable, d'un expert judiciaire, d'un consultant en informatique, d'un avocat, d'un consultant en relations publiques pour mener une analyse afin d'enquêter pour déterminer la cause et l'étendue d'une violation de données ou d'un piratage ainsi que la restauration des données et des systèmes informatiques perdus ou compromis.

Le système informatique désigne tout ordinateur, matériel, logiciel, application, processus, code, programme, technologie de l'information, système de communication ou dispositif électronique. Cela inclut tout système similaire et tout dispositif ou système associé d'entrée, de sortie ou de stockage de données, équipement de mise en réseau ou installation de sauvegarde.

Le réseau informatique désigne un groupe de systèmes informatiques et d'autres dispositifs électroniques ou installations de réseau reliés par une forme de technologie de communication, y compris l'Internet, intranet et les réseaux privés virtuels (VPN), permettant aux dispositifs informatiques en réseau d'échanger des données électroniques.

Les Informations commerciales confidentielles désignent toute information commerciale non publique d'un tiers, qu'elles soient cryptées ou non, qui ne peuvent pas être légalement obtenues ou connues du grand public, notamment les secrets commerciaux, les listes de clients, les dessins, les informations financières et les plans de marketing qui sont fournis à l'assuré par un tiers.

Dans le champ des cyber-attaques, le secteur de l'assurance a défini la cyber interruption des activités où l'assureur remboursera à l'assuré le manque à gagner et les dépenses opérationnelles pendant la période de restauration directement causée par un réseau malveillant et qui a causé une interruption partielle ou totale du réseau, ou un arrêt

[35] https://www.eiopa.europa.eu/topics/cyber-insurance_en

volontaire du système informatique de l'assuré lorsque cette action est prise pour minimiser, éviter ou atténuer un événement de sécurité ; ou exigé un arrêt réglementaire du Système informatique de l'Assuré lorsque cette mesure est ordonnée par un organisme de réglementation ou un organisme gouvernemental dans le cadre d'une Procédure réglementaire ou d'une Procédure RGPD.

Un virus est défini par le secteur de l'assurance comme tout code logiciel malveillant, y compris, mais sans s'y limiter, toute bombe logique, *ransomware,* ou « cheval de Troie » qui a été introduit par un tiers ou par un employé et qui est conçu pour endommager, détruire, corrompre, surcharger, contourner ou altérer la fonctionnalité des systèmes informatiques ou du réseau informatique.

La perte d'interruption d'activité cybernétique comme désignant la perte de profit et les dépenses opérationnelles de l'Assuré pendant la Période de Restauration résultant de l'interruption des activités de l'Assuré activités commerciales de l'Assuré.

La menace d'extorsion cybernétique en tant que menace raisonnablement crédible ou une série de menaces reliées entre elles (lancer une attaque par déni de service, diffuser, divulguer ou utiliser de façon inappropriée tout renseignement personnel obtenu à la suite de l'accès non autorisé au système informatique de l'assuré, et/ou crypter ou rendre autrement inaccessibles les données électroniques).

Le cyber-terrorisme comme l'utilisation de la technologie de l'information pour exécuter des attaques ou des menaces par toute personne ou tout groupe, qu'il agisse seul, au nom de, ou en relation avec, un individu, organisation ou gouvernement, dans l'intention de causer des dommages, d'intimider toute personne ou entité et/ou de détruire ou d'endommager des infrastructures ou des données critiques.

La Violation de données comme l'acquisition non autorisée par un tiers ou la perte de données, dont un cadre dirigeant a eu connaissance pour la première fois pendant la période d'assurance, qui compromet la sécurité, la confidentialité et/ou l'intégrité de données personnelles ou d'informations commerciales confidentielles détenues par l'assuré.

L'attaque par déni de service est une attaque mise en œuvre sur un réseau ou sur Internet destinée à perturber le fonctionnement normal d'un système informatique, et à rendre ce système inaccessible aux utilisateurs autorisés.

La perte de revenu d'entreprise dépendante comme la perte d'interruption d'activité cybernétique (à l'exclusion de toute responsabilité à l'égard du prestataire de services lui-même) subie par l'assuré en conséquence direct d'une compromission du réseau.

Les biens numériques désignent les Données Electroniques, les Logiciels, les fichiers audio et les fichiers images stockés sur le Système informatique de l'Assuré. A condition toujours que les Actifs Numériques ne comprennent pas les comptes, les factures, les preuves de dettes, l'argent, le matériel de clé cryptographique permettant l'accès aux monnaies numériques, les papiers de valeur, les registres, les résumés, les manuscrits d'actes ou autres documents, sauf s'ils ont été convertis en données électroniques et uniquement sous cette forme.

Les données électroniques désignent les informations utilisées, consultées, traitées, transmises ou stockées par un système informatique. La procédure RGPD est défini comme une enquête formelle menée par un organisme administratif ou réglementaire ou par un organisme gouvernemental similaire, en ce qui concerne une violation réelle ou présumée du RGPD par l'Assuré. Le cyber-attaquants est entendu comme toute personne, y compris un employé de l'Assuré, qui cible malicieusement l'Assuré et obtient un accès non autorisé à son Système Informatique, uniquement en contournant électroniquement les systèmes de sécurité mis en place pour se protéger contre un tel accès ou une telle utilisation non autorisés.

L'attaque de piratage désigne toute attaque électronique malveillante ou non autorisée, y compris, mais sans s'y limiter, toute signature électronique frauduleuse, tout acte de piratage ou de fraude., toute signature électronique frauduleuse, toute attaque par force brute, tout hameçonnage, toute attaque par déni de service, qui a été initiée par des tiers ou par des employés et qui est conçue pour endommager, détruire, corrompre, surcharger, contourner ou altérer la fonctionnalité des systèmes informatiques ou du réseau informatique.

Le logiciel malveillant ou mécanisme similaire désigne tout code de programme, toute instruction de programmation ou tout autre ensemble d'instructions construit intentionnellement avec la capacité d'endommager, d'interférer avec ou de nuire d'une autre manière, d'infiltrer ou de surveiller des programmes, des fichiers de données ou des opérations informatiques (qu'ils soient auto-répliqués ou non), y compris, mais sans s'y limiter, les virus, les chevaux de Troie, les vers, les bombes logiques, les rançongiciels, le déni d'accès ou le déni de service.

La compromission d'un réseau représente tout accès non autorisé, utilisation ou mauvaise utilisation, modification du système informatique, ou attaque par déni de service par un tiers ou un employé malveillant par le biais de tout moyen électronique, y compris, mais sans s'y limiter, les logiciels malveillants ou mécanismes similaires, virus, vers et chevaux de Troie, logiciels espions et logiciels publicitaires, attaques de type "zero-day", attaques de pirates informatiques et attaques par déni de service.

L'erreur d'exploitation désigne tout acte, erreur ou omission accidentelle, non intentionnelle ou négligent de la part d'un employé ou d'un tiers fournissant des services à l'Assuré dans l'exploitation du Système Informatique de l'Assuré.

Les frais d'exploitation représentent l'ensemble des frais raisonnables de location d'équipements informatiques supplémentaires et d'autres services supplémentaires, engagés afin de minimiser la perte de profit causée par une compromission du réseau.

La période de rétablissement représente la période qui commence dès qu'il y a eu une interruption de l'activité cybernétique qui a duré plus longtemps que la période de rétention et qui a été causée par une compromission du réseau.

Dans le champ de la protection des données, cibles récurrentes des cyber-attaques, les assureurs définissent un acte répréhensible en matière de confidentialité et de sécurité signifie comme le fait de ne pas protéger raisonnablement les Données Personnelles ou les informations commerciales confidentielles, la violation de toute loi, statut, règlement

régissant l'authenticité, la disponibilité, confidentialité, le stockage, le contrôle, la divulgation ou l'utilisation des données personnelles ; la violation d'une loi, d'un statut ou d'un règlement qui exige de l'assuré de fournir une notification aux personnes concernées par une violation de données ; la négligence entraînant l'impossibilité d'empêcher la compromission d'un réseau qui a pour conséquence l'impossibilité pour un utilisateur tiers autorisé d'accéder au système informatique de l'assuré, l'ajout, la modification, la copie, la destruction, l'effacement, la divulgation, l'endommagement, la suppression ou le vol de données résidant dans le système informatique de l'assuré, l'attaque par déni de service émanant du système informatique de l'assuré qui endommage, détruit le matériel, les programmes informatiques ou les données électroniques d'un tiers ou la transmission de logiciels malveillants à des tiers à partir du système informatique de l'assuré.

L'amende réglementaire est une amende civile assurable ou une sanction pécuniaire civile imposée par une autorité gouvernementale ou réglementaire pour une violation de données.

L'enquête réglementaire signifie enfin que l'assureur paiera les frais de défense et les amendes réglementaires (lorsqu'elles sont assurables par la loi) à la suite d'une enquête écrite, réelle ou imminente, menée par un organisme de réglementation ou une autorité gouvernementale sur un acte répréhensible réel ou présumé en matière de confidentialité et de sécurité causé par l'assuré, qui peut entraîner des conséquences négatives pour l'assuré.

Exemple de garanties proposées :

- Assistance et gestion de crise :
  - o un expert informatique est démarché pour déterminer la cause et l'étendue de l'attaque. Il détermine également la capacité de l'assuré à éviter ce futur incident.
  - o Un avocat détermine s'il peut appliquer la loi sur la Notification. Il aide également l'assuré lors d'une violation d'un contrat marchand et de récupération des coordonnées bancaires.
  - o Notification aux individus s'étant fait violer leurs données personnelles.
  - o Surveillance sur Internet sur les apparitions des données personnelles qui ont pu être volées.
- Responsabilité civile : L'assurance prend en charge les conséquences pécuniaires et les frais de défense si l'assuré à subi :
  - o Atteinte aux données
  - o Atteinte aux systèmes
  - o Non-respect d'une charte de protection des données
- Responsabilité liée au contenu d'un site internet : L'assurance prend en charge les conséquences pécuniaires et les frais de défense si l'assuré à subi :
  - o Diffamation, injure, atteinte à la réputation
  - o Atteinte au respect de la vie privée et au droit d'image
  - o Appropriation illégale d'un nom ou d'une image dans un but commercial
  - o Plagiat, piratage
  - o Contrefaçon d'un droit d'auteur (nom de domaine, logo, metatag).
  - o Usage d'un hyperlien en profondeur ou framing d'un contenu internet.
- Relations publiques : L'assurance paie les consultants en gestion de crise, la diffusion de messages publics
- Enquêtes administratives : L'assurance paie les frais de défense liés à la réclamation auprès de la CNIL (et des CNIL étrangères) lors d'une cyber-attaque.
- Pénalités PCI-DSS : sont prises en charge par l'assurance
- Cyber extorsion (rançongiciels) : l'assurance prend en charge :
  - o Tout paiement ou toute remise de biens fait sous la contrainte, par ou pour le compte de la société souscriptrice.
  - o Toute perte, destruction, disparition des espèces et biens en cours de transfert alors qu'ils seraient convoyés par toute autre personne autorisée par ou pour le compte de la société souscriptrice à cette fin.
  - o Les frais et honoraires payés par ou pour le compte de la société souscriptrice à des consultants en sécurité.
  - o Devoirs pour souscrire à cette assurance :
  - o Cette assurance fonctionne si le tiers effectuant la menace d'extorsion n'est pas salarié ou dirigeant de la société souscriptrice, ou qu'il n'agit pas en collusion avec eux.
  - o La société doit aussi prouver que le transfert s'est produit sous la contrainte.
  - o L'assureur doit pouvoir avertir la police de la menace d'extorsion.
  - o L'assuré doit maintenir la garantie cyber extorsion confidentielle. L'assureur peut résilier l'assurance sous 10 jours si la garantie est révélée à un tiers.
  - o Obligation de la société de souscription d'enquêter sur les menaces d'extorsion et d'éviter ou de limiter les coûts.
- Reconstitution des données : Assurance prend en charge les frais de reconstitution des données si
  - o Altération, infection, destruction, suppression ou endommagement d'une donnée protégée

o Incapacité d'accéder à une donnée protégée.

- Perte d'exploitation : Assurance prend en charge les pertes de revenus et dépenses supplémentaires au cours d'une période d'interruption (pas au-delà des 60 jours) de l'assurée lors d'une cyber-attaque. + (ne fonctionne pas si le sinistre dépend d'une responsabilité envers un tiers).

Ces garanties s'appliquent à l'encontre de tout assuré, dans le monde entier -> sauf sur les réclamations portant sur l'application du droit des États-Unis d'Amérique et du Canada.

Clause « Modification du risque en cours de contrat » : « Conformément aux dispositions de l'article L.113-2 du Code des assurances, le souscripteur est tenu de déclarer à l'assurer en cours de contrat les circonstances nouvelles qui ont pour conséquence soit d'aggraver les risques soit d'en créer de nouveaux et qui rendent de ce fait inexactes ou caduques les réponses faites à l'assureur ». « Le souscripteur doit, par lettre recommandée, déclarer ces circonstances à l'assureur dans les 15 jours à compter du moment où il en a connaissance. A défaut, il sera déchu de tout droit à garanti, à condition que l'assureur démontre que ce non-respect lui a causé un préjudice. »

Auditions

12 avril 2021 – Direction générale du Trésor :
M. Lionel Corre, Sous-directeur des assurances ;
M. Julien Dumond, Chef du bureau des produits et marchés d'assurance ;
Mme Mylène Larbi, Adjointe au chef de bureau Entreprises et intermédiaires d'assurance ;
M. Fouad Larhib, Adjoint au chef des produits et marchés d'assurance ;
M. Martin Landais, Chef du bureau Entreprises et intermédiaires d'assurance ;
M. Baptiste Ledan, Conseiller parlementaire et relations institutionnelles.

04 mai 2021 – Fédération française de l'assurance (FFA) :
M. Christophe Delcamp, Directeur adjoint assurances de biens et de responsabilités
Mme Flora Guillier, Chargée cyber à la direction assurances de biens et de responsabilités
Mme Clémence Heems, Chargée de mission affaires parlementaires
M. Franck Le Vallois, Directeur général de la Fédération française de l'assurance
Mme Viviana Mitrache, Sous-Directrice, responsable du département des affaires parlementaires
Mme Anne-Marie Papeix, Chargée cyber à la direction assurances de biens et de responsabilités

05 mai 2021 – Cybermalveillance
M. Jérôme Notin, Directeur général de cybermalveillance

06 mai 2021– Autorité de contrôle prudentiel et de résolution (ACPR) :
Mme Véronique Bensaid-Cohen, Conseillère Parlementaire auprès du Gouverneur
Mme Emilie QUEMA, Directrice des contrôles spécialisés et transversaux

11 mai 2021 – Caisse centrale de réassurance (CCR) :
M. Bertrand Labilloy, Directeur général

12 mai 2021 – Hiscox
M. Fréderic Rousseau, expert marché Cyber sécurité

12 mai 2021 – Association des Professionnels de la Réassurance en France (APREF) :
M. Nicolas BOUDIAS, Directeur général
M. Walter ERAUD, membre du comité directeur de l'APREF
M. Bertrand ROMAGNE, Président

19 mai 2021 – Gras Savoye :
M. Guillaume Deschamps, Directeur exécutif, chef de la division France, Russie et Europe centrale et orientale des Risques financiers, exécutifs et professionnels
M. Ezechiel Symenouh, expert cyber à la division Risque financier, exécutif et professionnel

20 mai 2021 - Fédération des Garanties et Assurances Affinitaires (FG2A) :
Me Géraldine Brasier Porterie, Membre
M. Patrick Raffort, Président-fondateur
Me Benoit Lapointe de Vaudreuil, Vice-Président

20 mai 2021 – Institut des actuaires :
Mme Caroline Hillairet, Membre
M. Olivier Lopez, Directeur
Mme Florence Picard, Membre du Haut Conseil et Présidente Jury et groupes Cyber Risk, Big Data et Blockchain
M. Philippe Talleux, Président

26 mai 2021 – SCOR :
M. Laurent Rousseau, Directeur général
M. Didier Parsoire, Directeur Cyber Solutions

26 mai 2021 – Association pour le Management des Risques et des Assurances de l'Entreprise (AMRAE) :
M. Hubert de L'ESTOILE, Directeur général

26 mai 2021 – AXA XL :
M. Stéphane Vauterin, Responsable France de la souscription lignes financières

27 mai 2021– Zurich :
Mme Anne Reynaud, Directeur juridique et Responsable de la conformité
Mme Florence Tondu-Mélique, Présidente-Directrice Générale France

01 juin 2021 – Partnerre :
M. Christopher Mc Evoy, Directeur risqué cyber
M. Jacques de Franclieu, Directeur France Assurance multirisques

02 juin 2021- August Debouzy :
Maitre Florence Chafiol

04 juin 2021– PwC :
Mme Pauline Adam-Kalfon, Directrice-associée Inclusion et Diversité

16 juin 2021 - Fédération nationale des syndicats à agents généraux d'assurance (AGEA) :
M. Pascal Chapelon, Président
M. Karl Westeel, Chargé de mission

16 juin 2021- RU'Safe :
M. Eric Gormand, Président directeur général

24 juin 2021 – QBE :
Mme Amanda Maréchal, Souscriptrice Cyber
Mme Françoise Mari, Directrice des Lignes Financières

28 juin 2021– Cyrating :
M. Christophe Ternat, Président-fondateur

30 juin 2021– Ecoter :
M. Alain Melka, Directeur Général des Services

01 juillet 2021 – Citalid :
M. Maxime Cartan, Président-fondateur
Mme Roxanne Deslandes, Chargée de la cyber-assurance

02 juillet 2021 – Chambre Nationale des Conseils Experts Financiers (CNCEF) :
M. Stéphane Fantuz, Président

02 juillet 2021 – Syndicat des Courtiers d'Assurance (SYCRA) :
M. Eric Lamouret, Président
M. Dominique Paliard, Vice-président

19 juillet 2021- Société mutuelle d'assurance des collectivités locales (SMACL) :
Mme Nathalie Bacquet, Administratrice
M. Jean-Luc de Boissieu, Président
Mme Mélissa Dernevaux, Responsable Innovation et intelligence des données

19 juillet 2021– Cycover :
M. Pierre Ekmekci, co-Fondateur

26 juillet 2021 - Comité stratégique de filière industrie de sécurité :
M. Jacques Roujansky, Délégué permanent

10 aout 2021 – AIAC :
M. Mathieu Joly, Courtier, Chargé de Clientèle Entreprise

10 aout 2021– Confédération des petites et moyennes entreprises (CPME) :
M. Marc Bothorel, Membre de la Commission numérique
Mme Delphine Borne, Chargé de mission au sein de la direction des affaires économiques, juridiques et fiscales
Mme Stéphanie Pauzat, Vice-présidente déléguée

01 septembre 2021 – Wavestone :
M. Gérome Billois, Associé cybersécurité

14 septembre 2021 – Agence nationale de la sécurité des services d'informations (ANSSI) :
M. Guillaume Poupard, Directeur général